

Forum:[Hack Forums](#)

Thread: [Blaqk the master reverse engineer](#)

N3xtSolutions - June 12, 2022, 10:42 am

ID: 969496831056838706

<https://gyazo.com/70e9a1e0726e423cbb9a18ec7ea0f63a>

I really didn't want to spend any time on this but, here we go i guess.

The so-called ESEA/FaceIT proof undetected cheat made by the highly skilled reverse engineer(13 years) @blaqk (uid=5207384) using an undisclosed ring3 exploit!

Our journey starts with vitamin.exe

This is a .net application that takes an array of bytes(in memory already) and uses runPE to inject into cmd.

This array of bytes happens to be a valid PE image out of the box(shocker)

<https://gyazo.com/372b727b1e869cf1f22d9158526127c1>

<https://gyazo.com/eba0f35f090965b2a2126b38e690a1af>

This is the module that does all the undetectable super-secret ring3 exploit stuff.

Let's look at the imports:

<https://gyazo.com/842de530edc217ec8dffde14b6fcd459>

<https://gyazo.com/7a496c6ebcde89d0d220e7c2570fb567>

Interesting... secret sauce is maybe a pixel bot?

Here is the main logic:

<https://gyazo.com/716c8c54193a657c71fc2b991934a7ff>

For those who are not familiar with what you see:

All this does is gets the current cursor position, checks the pixel it is pointing at, and if it matches the desired parameters,

it calls SystemParametersInfo with 0x0071 flag which is SPI_SETMOUSESPEED to change mouse sensitivity.

An aim squeeze(that's what he calls this). It will lower your mouse sensitivity when on an enemy target.

So in conclusion, this is just a quick scam for people to test and get banned after a couple of days. (after paying for the cheat)

Be smart, don't be like this guy.

SSH - June 12, 2022, 3:05 pm

High quality post, I like it.

SIM-5049184 - June 12, 2022, 8:54 pm

Ah, as I presumed. Thanks

blaqk - June 12, 2022, 10:31 pm

You have to give admiration for my work though because my work has been undetected for more than year. I knew this was coming but I will stand strong. I knew there was something shady about you but who cares. Good job. I laughed so hard when you said this will get you banned cause it won't. Remember what I gave you was a test cheat not the full cheat ;)

I also have to express the fact that you called my cheat "a quick scam" which it is not. This cheat has been undetected ever since I created it. I think this is just quick way for you to discredit me in order to gain trophy points. My cheat is not a scam and it is indeed undetected :)

Riveryes - June 13, 2022, 11:37 pm

This all reminds me of leaguecheat or the esea glow hack from this german/ukrainian guy.

Legitsense

biscuit deluxe - June 14, 2022, 6:31 pm

(Jun 12, 2022 10:31 PM)blaqk Wrote: [\[CITE\]](#) You have to give admiration for my work though because my work has been undetected for more than year. I knew this was coming but I will stand strong. I knew there was something shady about you but who cares. Good job. I laughed so hard when you said this will get you banned cause it won't. Remember what I gave you was a test cheat not the full cheat ;)

I also have to express the fact that you called my cheat "a quick scam" which it is not. This cheat has been undetected ever since I created it. I think this is just quick way for you to discredit me in order to gain trophy points. My cheat is not a scam and it is indeed undetected :)

Ah yes, the classic "test cheat."

MindkcuF - June 14, 2022, 9:03 pm

I do like how the guy claims to have given you "half" the cheat after you call him out for blatantly talking shit. Good job

Menalix - June 14, 2022, 10:01 pm

(Jun 14, 2022 06:31 PM)biscuit deluxe Wrote: [\[CITE\]](#) Ah yes, the classic "test cheat." hahahah ? so classic

blaqk - June 14, 2022, 10:24 pm

(Jun 14, 2022 09:03 PM)MindkcuF Wrote: [\[CITE\]](#) I do like how the guy claims to have given you "half" the cheat after you call him out for blatantly talking shit. Good job

I hardly think so. If you read his post properly you will know I was not talking rubbish. The cheat actually works and my method of initiating the cheat into memory is out of the box and will evade the anti-cheats scan. The cheat I gave him was indeed a test version and not the full cheat for obvious reasons.

(Jun 14, 2022 10:01 PM)Menalix Wrote: [\[CITE\]](#) hahahah ? so classic
Hey Menalix. Big fan :)

MindkcuF - June 14, 2022, 10:30 pm

(Jun 14, 2022 10:24 PM)blaqk Wrote: [\[CITE\]](#) I hardly think so. If you read his post properly you will know I was not talking rubbish. The cheat actually works and my method of initiating the cheat into memory is out of the box and will evade the anti-cheats scan. The cheat I gave him was indeed a test version and not the full cheat for obvious reasons.

Did he pay for this fake test version you gave him, or did he pay for your "real" cheat and never got what he paid for then?

I only ask as he does mention he paid for your cheat, why are you selling test versions

blaqk - June 14, 2022, 10:54 pm

(Jun 14, 2022 10:30 PM)MindkcuF Wrote: [\[CITE\]](#) Did he pay for this fake test version you gave him, or did he pay for your "real" cheat and never got what he paid for then?

I only ask as he does mention he paid for your cheat, why are you selling test versions

Nope he didn't pay anything for the test cheat. If he had paid he would have had the full cheat. If he had mentioned that he paid for the cheat then he is lying and has no place on this forum as he is spreading misinformation.

MindkcuF - June 14, 2022, 10:55 pm

(Jun 14, 2022 10:54 PM)blaqk Wrote: [\[CITE\]](#) Nope he didn't pay anything for the test cheat. If he had paid he would have had the full cheat. If he had mentioned that he paid for the cheat then he is lying and has no place on this forum as he is spreading misinformation.

I believe i miss read it when he mentioned "paying", he isn't spreading misinformation he told us what your "test" cheat does.

blaqk - June 14, 2022, 10:59 pm

(Jun 14, 2022 10:55 PM)MindkcuF Wrote: [\[CITE\]](#) I believe i miss read it when he mentioned "paying", he isn't spreading misinformation he told us what your "test" cheat does.

I used to give all my clients a test cheat for the day for free but obviously had to cut that out. Yes he is explaining roughly how the test cheat works but the full version does so much more.

N3xtSolutions - June 14, 2022, 11:06 pm

(Jun 14, 2022 10:24 PM)blaqk Wrote: [\[CITE\]](#) I hardly think so. If you read his post properly you will know I was not talking rubbish. The cheat actually works and my method of initiating the cheat into memory is out of the box and will evade the anti-cheats scan. The cheat I gave him was indeed a test version and not the full cheat for obvious reasons.

Hey Menalix. Big fan :)

Hey guys, I discovered runPE!!! very unique much undetected!!

You are insignificant, please move along

Menalix - June 14, 2022, 11:16 pm

(Jun 14, 2022 10:24 PM)blaqk Wrote: [\[CITE\]](#) I hardly think so. If you read his post properly you will know I was not talking rubbish. The cheat actually works and my method of initiating the cheat into memory is out of the box and will evade the anti-cheats scan. The cheat I gave him was indeed a test version and not the full cheat for obvious reasons.

What makes you think it evade anti-cheat scans?

RunPE evades anti-virus callbacks for file creation, most anti-cheats doesn't have file creation callbacks.

It doesn't make the memory mapping the data reside in unscannable.

Idk what faceit and esportal do to prevent pixelbots. But ESEA will always catch most, prolly anything when ring3, they log a lot of stuff, enough reports and they'll take a look.

It's better to just state what your cheat is, instead of using false marketing.

blaqk - June 14, 2022, 11:17 pm

(Jun 14, 2022 11:06 PM)N3xtSolutions Wrote: [\[CITE\]](#) Hey guys, I discovered runPE!!! very unique much undetected!!

You are insignificant, please move along

Yes RunPE is common but the way I do it is unique and undetected. I guess you're here to discredit me even more to gain additional trophy points. Insignificant? I hardly think so.

N3xtSolutions - June 14, 2022, 11:31 pm

(Jun 14, 2022 11:17 PM)blaqk Wrote: [\[CITE\]](#) Yes RunPE is common but the way I do it is unique and undetected. I guess you're here to discredit me even more to gain additional trophy points. Insignificant? I hardly think so.

Okay. Let look at "your" way.

<https://pastebin.com/fztX1Ain>

Can you point out what is unique?

blaqk - June 14, 2022, 11:36 pm

(Jun 14, 2022 11:16 PM)Menalix Wrote: [\[CITE\]](#) What makes you think it evade anti-cheat scans? RunPE evades anti-virus callbacks for file creation, most anti-cheats doesn't have file creation callbacks.

It doesn't make the memory mapping the data reside in unscannable.

Idk what faceit and esportal do to prevent pixelbots. But ESEA will always catch most, prolly anything when ring3, they log a lot of stuff, enough reports and they'll take a look.

It's better to just state what your cheat is, instead of using false marketing.

Menalix my cheat is in fact roughly a pixelbot and it has something to do with your sensitivity. My goal was never to actually touch anything in the games memory as you know better than most is flawless if you know what you're doing. Most cheats similar to mine, hooks the games window and takes screenshots and then moves your mouse to the desired color. Which is in fact a red flag for anti-cheats obviously and they'll block your attempts at taking screenshots but you can too bypass this by running obs as it does have a valid handle. You're right. If it is blatant you will get reported and they'll do their manual analysis. I can assure my cheat does not do anything publicly known and the way the cheat initiates into memory is everything. The cheat itself is just the "sauce" but the way it initiates into memory is my secret recipe.

(Jun 14, 2022 11:31 PM)N3xtSolutions Wrote: [\[CITE\]](#) Okay. Let look at "your" way.

<https://pastebin.com/fztX1Ain>

Can you point out what is unique?

Do you honestly think I was gonna give you my full cheat without paying for it? The full cheat is completely different. Non of what I gave you is my actual methods as the cheat was a trial version. So you can show everyone the source codes it won't make a difference xD I'll give you the full cheat to see what your're brilliant mind can do to reverse it?

N3xtSolutions - June 15, 2022, 12:24 am

(Jun 14, 2022 11:36 PM)blaqk Wrote: [\[CITE\]](#) ...

Do you honestly think I was gonna give you my full cheat without paying for it? The full cheat is completely different. Non of what I gave you is my actual methods as the cheat was a trial version. So you can show everyone the source codes it won't make a difference xD I'll give you the full cheat to see what you're brilliant mind can do to reverse it?

Oh, so you were giving your potential customers a shitty, detected cheat for them to try?

blaqk - June 15, 2022, 12:33 am

(Jun 15, 2022 12:24 AM)N3xtSolutions Wrote: [\[CITE\]](#) Oh, so you were giving your potential customers a shitty, detected cheat for them to try?

Nope. They were able to test it while playing on esea and faceit for the day without any issues :)

N3xtSolutions - June 15, 2022, 12:38 am

(Jun 15, 2022 12:33 AM)blaqk Wrote: [\[CITE\]](#) Nope. They were able to test it while playing on esea and faceit for the day without any issues :)

I mean, that's what you just said. Your trial cheat doesn't have "secret" "undetectable" memory stuff that you are doing? So that means you are giving your potential customers the shitty runPE to get fucked?

blaqk - June 15, 2022, 12:49 am

(Jun 15, 2022 12:38 AM)N3xtSolutions Wrote: [\[CITE\]](#) I mean, that's what you just said. Your trial cheat doesn't have "secret" "undetectable" memory stuff that you are doing? So that means you are giving your potential customers the shitty runPE to get fucked?

Nope this trial version was more than safe and undetected up until you decided to scam me and rant on a public forum, discrediting me to gain trophy points. Obviously I cannot give my clients a trial anymore. Thank God I wasn't stupid enough to give you my full cheat.

DanketyDank - June 15, 2022, 11:39 pm

(Jun 15, 2022 12:49 AM)blaqk Wrote: [\[CITE\]](#) Nope this trial version was more than safe and undetected up until you decided to scam me and rant on a public forum, discrediting me to gain trophy points. Obviously I cannot give my clients a trial anymore. Thank God I wasn't stupid enough to give you my full cheat.

No it was not more than safe. Come on man, its shown right here what it does - its not safe, never was.

Constantly saying that you have this full cheat seems like a trick to just get someone buy it. But maybe you do actually have and its working as you say, if so - good job on that. But dont call this leaked one safe, its not

blaqk - June 16, 2022, 1:30 am

(Jun 15, 2022 11:39 PM)DanketyDank Wrote: [\[CITE\]](#) No it was not more than safe. Come on man, its shown right here what it does - its not safe, never was.

Constantly saying that you have this full cheat seems like a trick to just get someone buy it. But maybe you do actually have and its working as you say, if so - good job on that. But dont call this leaked one safe, its not

This was safe to TEST and was not intended as the finished product. As I did state it was good to use for a day. My full version is completely different and does have my actual methods. My intent now is to not let any of my clients use the test cheat anymore for obvious reason. Any of my new clients will be receiving the full version :)

Riveryes - June 16, 2022, 11:19 am

Ghostware mixxed with legitsense

baka~ - June 17, 2022, 12:28 am

This reminds me of the golden times in this section.

biscuit deluxe - June 17, 2022, 2:48 pm

(Jun 17, 2022 12:28 AM)baka~ Wrote: [\[CITE\]](#) This reminds me of the golden times in this section.
Vuno moment

Lilith - June 17, 2022, 6:15 pm

(Jun 17, 2022 12:28 AM)baka~ Wrote: [\[CITE\]](#) This reminds me of the golden times in this section.
Miss the drama Tristan would bring

blaqk - June 20, 2022, 8:27 am

[New cheat available :\)](#)

Exca h - June 20, 2022, 11:35 am

Ah, as I presumed. Thanks

supex0 - June 23, 2022, 10:28 am

(Jun 17, 2022 02:48 PM)biscuit deluxe Wrote: [\[CITE\]](#) Vuno moment exactly.

blaqk - June 23, 2022, 12:15 pm

(Jun 23, 2022 10:28 AM)supex0 Wrote: [\[CITE\]](#) exactly.
Hey supex0. Big fan :)